Rec'd PCT/PTO 08 JUL 2004

10/500930

PATENT COOPERATION TREATY

PCT

REC'D 19 APR 2004

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference S0049PCT	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FI 03/00045	International filing date *(day/month/year)* 21.01.2003	Priority date *(day/month/year)* 22.01.2002
International Patent Classification (IPC) or both national classification and IPC H04L29/06		
Applicant INTRASECURE NETWORKS OY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 19.08.2003	Date of completion of this report 16.04.2004
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Kopp, K Telephone No. +49 89 2399-7833

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-38 as originally filed

Claims, Numbers

1-26 filed with telefax on 17.03.2004

Drawings, Sheets

1/6-6/6 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	3,6,11,12,13,14,15,16,17,18,19,20,21
	No:	Claims	1,2,4,5,7,8,9,10,22,23,24,25,26
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-26
Industrial applicability (IA)	Yes:	Claims	1-26
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The following documents (D) are mentioned:

   D1: US 2001/047487 A1 (LINNAKANGAS TOMMI ET AL) 29 November 2001 (2001-11-29)
   D2: US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19)
   D3: WO 00 78008 A (SSH COMM SECURITY LTD ;KIVINEN TERO (FI); YLOENEN TATU (FI)) 21 December 2000 (2000-12-21)
   D4: US 2001/020273 A1 (MURAKAWA YASUSHI) 6 September 2001 (2001-09-06)

2. Claim 22 lacks novelty (Article 33(2) PCT).

2.1 Document D1, which is considered to represent the most relevant state of the art for claim 1, discloses according to the subject-matter of claim 1:

- Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer (paragraph 24, lines 4-8)

characterized in that

- the first and the second computers have means to perform IPSec processing (paragraph 24, lines 4-8),
- and the intermediate computer have translation tables to perform IPSec and IKE translation (paragraph 24, lines 11-15).

3. The features of independent claim 22 are also disclosed in any of D2 (see e.g. figures 1, 5; paragraphs 4, 5, 48), D3 (see e.g. page 3, line 24 - page 4, line 10; page 9, lines 7 - 13; figures 1a, 1b, 3) and D4 (see e.g. paragraphs 71-76).

4. If novelty were disputable based on minor differences of interpretation, it is pointed out that the subject-matter of claim 22 would still not involve an inventive step (Article 33(3) PCT).

5. The subject-matter of independent method claim 1 corresponds to the subject-matter of independent apparatus claim 22. Thus, claim 1 also lacks novelty (Article 33(2) PCT).

6. Dependent claims do not contain any subject-matter which, in combination with the subject-matter to which they refer, meet the requirements of the PCT in respect of novelty and inventive step (Article 33(2) and (3) PCT). They are either disclosed in D1 (e.g. "the secure message is formed by using an IPSec connection between the first computer and the second computer"; "preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol"), in D2 (e.g "the request for registration is encrypted") or common measures (e.g. "forwarding of the message is performed by making use of the SSL or TLS protocols"; "the secure message is sent using IPSec tunnel mode"; "the secure message is sent using IPSec transport mode") obvious for a person skilled in the art.

Rec'd PCT/PTO 08 JUL 2004

10/500930

REPLACED BY ART 34 AMDT

CLAIMS

1. Method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network, characterized by
   a) forming a message in the first computer or in a computer that is served by the first computer, and in the latter case sending the message to the first computer,
   b) in the first computer, forming a secure message by giving the message a unique identity and a destination address,
   c) sending the message from the first computer to the intermediate computer,
   d) using said destination address and the unique identity to find an address to the second computer,
   e) substituting the current destination address with the found address to the second computer,
   f) substituting the unique identity with another unique identity,
   g) forwarding the message to the second computer.

2. Method of claim 1, characterized in that the secure forwarding of the message is performed by making use of the IPSec protocols, whereby the secure message is formed in step b) by using an IPSec connection between the first computer and the second computer formed for this purpose in the method.

3. Method of claim 1, characterized in that the secure forwarding of the message is performed by making use of the SSL or TLS protocols.

4. Method of claim 2, characterized in that a preceding distribution of keys to the components for forming the IPSec connection is performed manually.

5. Method of claim 2, characterized in that a preceding distribution of keys for forming the IPSec connection is performed by an automated key exchange protocol.

6. Method of claim 5, c h a r a c t e r i z e d in that the automated key exchange protocol between the first computer and the second computer is performed by means of a modified IKE key exchange protocol between the first computer and the intermediate computer and a standard IKE key exchange protocol between the intermediate computer and the second computer.

7. Method of any of claims 2, 5 or 6, c h a r a c t e r i z e d in that the message that is sent from the first computer in step c) is a packet and contains message data, an inner IP header containing the actual sender and receiver addresses, an outer IP header containing the addresses of the first computer and the intermediate computer, a unique identity, and other security parameters.

8. Method of any of claims 2, 5 or 6, c h a r a c t e r i z e d in that that the IPSec connection is one or more security associations (SA) and the unique identity is one or more SPI values and the other security parameters include the sequence number(s).

9. Method of any of claims 1 – 8, c h a r a c t e r i z e d in that the matching in step d) is performed by means of a translation table stored at the intermediate computer.

10. Method of any of claims 1 - 9, c h a r a c t e r i z e d in that both the address and the SPI-value are changed by the intermediate computer in steps e) respective f).

11. Method of any of claims 1 - 10, c h a r a c t e r i z e d in that the first computer is a mobile terminal, whereby the mobility is enabled by modifying the translation table at the intermediate computer.

12. Method of claim 11, c h a r a c t e r i z e d in that said modification of the translation tables is performed by sending a request for registration of the new address from the first computer to the intermediate computer, and optionally, by sending a registration reply from the intermediate computer to the first computer.

13. Method of claim 12, c h a r a c t e r i z e d in that the registration and/or reply is authenticated and/or encrypted by IPSec.

14. Method of any of claims 4 -13, c h a r a c t e r i z e d in that the key distribution for the secure connections is established by establishing an IKE protocol translation table, and using the translation table to modify IP addresses and cookie values of IKE packets in the intermediate computer.

15. Method of claim 14, c h a r a c t e r i z e d in that the key exchange distribution is established by
generating an initiator cookie and sending a zero responder cookie to the second computer,
generating a responder cookie in the second computer,
establishing a mapping between IP addresses and IKE cookie values in the intermediate computer,
using a translation table to modify IKE packets in flight by modifying the external IP addresses and possibly IKE cookies of the IKE packets.

16. Method of claim 14 or 15, c h a r a c t e r i z e d in that the modified IKE protocol between the first computer and the intermediate computer is modified such that the IKE keys are transmitted from the first computer to the intermediate computer for decryption and modification of IKE packets.

17. Method of claim 14 or 15, c h a r a c t e r i z e d in that in the modified IKE protocol between the first computer and the intermediate computer the modification of the IKE packets is done by the first computer with the intermediate computer requesting such modifications.

18. Method of claim 16, c h a r a c t e r i z e d in that the address is defined so that the first computer is identified for the second computer by the intermediate computer by means of an IP address taken from a pool of user IP addresses when forming the translation table.

19. Method of any of claims 1 -18, c h a r a c t e r i z e d in that the secure message is sent using IPSec transport mode.

20. Method of any of claims 1 -18, c h a r a c t e r i z e d in that the secure message is sent using IPSec tunnel mode.

21. Telecommunication network for secure forwarding of messages, comprising at least a first computer, a second computer and an intermediate computer, c h a r a c t e r i z e d in that the first and the second computers have means to perform IPSec processing, and the intermediate computer have means to perform IPSec translation.

22. Network of claim 21, c h a r a c t e r i z e d in that the intermediate computer furthermore has means to perform IKE translation.

23. Network of claim 21 or 22, c h a r a c t e r i z e d in that the means to perform IPSec translation and IKE translation consists of translation tables.

24. Network of claim 22, c h a r a c t e r i z e d in that the translation table for IPSec translation comprising IP addresses of the intermediate computer to be matched with IP addresses of the second computer.

25. Network of claim 22, c h a r a c t e r i z e d in that one of the mapping tables for IKE translation consists of two partitions, one for the communication between the first computer and the intermediate computer and another for the communication between the intermediate computer and the second computer.

26. Network of claim 25, c h a r a c t e r i z e d in that both partitions of the mapping table for IKE translation contains translation fields for the source IP address, the destination IP address, initiator and responder cookies between respective computers.

27. Network of claim 28, c h a r a c t e r i z e d in that there is another translation table for IKE translation containing fields for matching a given user to a given second computer.